

Effects of the LLL reduction on the success probability of the Babai point and on the complexity of sphere decoding

Xiao-Wen Chang, Jinming Wen, Xiaohu Xie

March 2, 2013

Abstract

The common method to estimate an unknown integer parameter vector in a linear model is to solve an integer least squares (ILS) problem. A typical approach to solving an ILS problem is sphere decoding. To make a sphere decoding algorithm faster, the well-known LLL reduction is often used as preprocessing. The Babai point produced by the Babai nearest plan algorithm is a suboptimal solution of the ILS problem. First we prove that the success probability of the Babai point as a lower bound on the success probability of the ILS estimator is sharper than the lower bound provided by Hassibi and Boyd [6]. Then we show rigorously that applying the LLL reduction algorithm will increase the success probability of the Babai point. Finally we show rigorously that applying the LLL-reduction algorithm will reduce the computational complexity of sphere decoders which is measured approximately by the number of nodes in the search tree in the literature.

1 Introduction

Consider the following linear model:

$$\mathbf{y} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{v}, \quad (1)$$

where $\mathbf{y} \in \mathbb{R}^n$ is an observation vector, $\mathbf{v} \in \mathbb{R}^n$ is a noise vector following the Gaussian distribution $\mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I})$ with σ being known, $\mathbf{A} \in \mathbb{R}^{m \times n}$ is a model matrix with full column rank, and $\hat{\mathbf{x}} \in \mathbb{Z}^n$ is an unknown integer parameter vector. A common method to estimate $\hat{\mathbf{x}}$ in (1) is to solve the following integer least squares (ILS) problem:

$$\min_{\mathbf{x} \in \mathbb{Z}^n} \|\mathbf{y} - \mathbf{A}\mathbf{x}\|_2^2, \quad (2)$$

whose solution \mathbf{x}^{ILS} is the maximum-likelihood estimator of $\hat{\mathbf{x}}$. The ILS problem is also referred to as the closest point problem in the literature as it is equivalent to find a point in the lattice $\{\mathbf{A}\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$ which is closest to \mathbf{y} .

A typical approach to solving (2) is the discrete search approach, referred to as sphere decoding in communications, such as the Schnorr-Euchner algorithm [14] or its variants, see for example [2, 4]. To make the search faster, a lattice reduction is performed to transform the given problem to an equivalent problem. The widely used reduction is the LLL-reduction proposed by Lenstra, Lenstra and Lovász in [10].

It has been shown that the ILS problem is NP-hard [18, 12]. Solving (2) may become time-prohibitive when \mathbf{A} is ill conditioned, the noise is large, or the dimension of the problem is large [8]. So for some applications, an approximate solution, which can be produced quickly, is computed instead. One often used approximate solution is the Babai point, produced by Babai's nearest plane algorithm [3]. This approximate solution is also the first integer point found by the Schnorr-Euchner algorithm. In communications, a method for finding this approximate solution is referred to as a successive interference cancelation decoder.

In order to verify whether an estimator is good enough for a practical use, one needs to find the probability of the estimator being equal to the true integer parameter vector, which is referred to as success probability [6]. The probability of wrong estimation is referred to as error probability, see, e.g., [7].

If the Babai point is used as an estimator of the integer parameter vector $\hat{\mathbf{x}}$ in (1), certainly it is important to find its success probability, which can easily be computed. But even if one intends to compute the ILS estimator, it is still important to find the success probability of the Babai point. It is very difficult to compute the success probability of the ILS estimator, so lower and upper bounds have been considered to approximate it, see, e.g., [6, 20]. In [17] it was shown that the success probability of the ILS estimator is the largest among all “admissible” estimators, including the Babai point, which is referred to as a bootstrap estimator in [17]. The success probability of the Babai point is often used as an approximation to the success probability of the ILS estimator. In general, the higher the success probability the Babai point, the lower the complexity of finding the ILS estimator by the discrete search approach. In practice, if the success probability of the Babai point is high, say close to 1, then one does not need to spend extra computational time to find the ILS estimator.

Numerical experiments have shown that after the LLL reduction, the success probability of the Babai point increases [5]. But whether the LLL reduction can always improve the success probability of the Babai point is still unknown. In this paper, we will prove that the success probability of the Babai point will become higher after the LLL-reduction algorithm is used. It is well-known that the LLL reduction can make sphere decoders faster. But to our knowledge there is still no rigorous justification. We will show that the LLL reduction can always decrease the computational complexity of sphere decoders, an approximation to the number of nodes in the search tree given in the literature.

The rest of the paper is organized as follows. In section 2, we introduce the LLL reduction to reduce the ILS problem 2. In section 3, we introduce the Babai point and a formula to compute the success probability of the Babai point. and we show that the success probability of the Babai point is a sharper lower bound on the success probability of ILS estimator compared with the lower bound given in [6]. In section 4, we rigorously prove that the LLL-reduction algorithm improve the success probability of the Babai point. In section 5, we rigorously show that the LLL reduction algorithm reduce the computational complexity of sphere decoders. Finally we summarize this paper in section 6.

For $\mathbf{x} \in \mathbb{R}^n$, we use $\lfloor \mathbf{x} \rfloor$ to denote its nearest integer vector, i.e., each entry of \mathbf{x} is rounded to its nearest integer (if there is a tie, the one with smaller magnitude is chosen). The success probabilities of the Babai point and the ILS estimator are denoted by P_B and P_{ILS} , respectively.

2 LLL Reduction and transformation of the ILS Problem

Assume that \mathbf{A} in the linear model (1) has the QR factorization

$$\mathbf{A} = [\mathbf{Q}_1, \mathbf{Q}_2] \begin{bmatrix} \mathbf{R} \\ \mathbf{0} \end{bmatrix},$$

where $[\mathbf{Q}_1, \mathbf{Q}_2] \in \mathbb{R}^{m \times m}$ is orthogonal and $\mathbf{R} \in \mathbb{R}^{n \times n}$ is upper triangular. Without lose of generality, we assume the diagonal entries of \mathbf{R} are positive throughout the paper. Define $\tilde{\mathbf{y}} = \mathbf{Q}_1^T \mathbf{y}$. From (1), we have $\tilde{\mathbf{y}} = \mathbf{R}\hat{\mathbf{x}} + \mathbf{Q}_1^T \mathbf{v}$. Because $\mathbf{v} \sim \mathcal{N}(\mathbf{0}, \sigma^2 \mathbf{I})$, it follows that $\tilde{\mathbf{y}} \sim \mathcal{N}(\mathbf{R}\hat{\mathbf{x}}, \sigma^2 \mathbf{I})$.

With the QR factorization of \mathbf{A} , the ILS problem (2) can be transformed to

$$\min_{\mathbf{x} \in \mathbb{Z}^n} \|\tilde{\mathbf{y}} - \mathbf{R}\mathbf{x}\|_2^2. \quad (3)$$

One can then apply a sphere decoder such as the Schnorr-Euchner search algorithm [14] to find the solution of (3).

The efficiency of the search process depends on \mathbf{R} . For efficiency, one typically uses the LLL reduction instead of the QR factorization. After the QR factorization of \mathbf{A} , the LLL reduction [10] reduces the matrix \mathbf{R} in (3) to $\bar{\mathbf{R}}$:

$$\bar{\mathbf{Q}}^T \mathbf{R} \mathbf{Z} = \bar{\mathbf{R}}, \quad (4)$$

where $\bar{\mathbf{Q}} \in \mathbb{R}^{n \times n}$ is orthogonal, $\mathbf{Z} \in \mathbb{Z}^{n \times n}$ is a unimodular matrix (i.e., $\det(\mathbf{Z}) = \pm 1$), and $\bar{\mathbf{R}} \in \mathbb{R}^{n \times n}$ is upper triangular with positive diagonal entries and satisfies the following conditions:

$$|\bar{r}_{ik}| \leq \frac{1}{2} \bar{r}_{ii}, \quad i = 1, 2, \dots, k-1 \quad (5)$$

$$\delta \bar{r}_{k-1,k-1}^2 \leq \bar{r}_{k-1,k}^2 + \bar{r}_{k,k}^2, \quad k = 2, 3, \dots, n, \quad (6)$$

where δ is a constant with $1/4 < \delta \leq 1$. The matrix \mathbf{R} is said to be δ -LLL reduced or simply LLL reduced. Equations (5) and (6) are referred to as the size-reduced condition and the Lovász condition, respectively.

The original LLL algorithm given in [10] can be described in the matrix language. Two types of basic unimodular matrices are implicitly used to update \mathbf{R} so that it satisfies the two conditions. One is the integer Gauss transformations (IGT) matrices and the other is permutation matrices, see below.

To meet the first condition in (5), we can apply an IGT, which has the following form:

$$\mathbf{Z}_{ik} = \mathbf{I} - \zeta \mathbf{e}_i \mathbf{e}_k^T.$$

Applying \mathbf{Z}_{ik} ($i < k$) to \mathbf{R} from the right gives

$$\bar{\mathbf{R}} = \mathbf{R} \mathbf{Z}_{ik} = \mathbf{R} - \zeta \mathbf{R} \mathbf{e}_i \mathbf{e}_k^T.$$

Thus $\bar{\mathbf{R}}$ is the same as \mathbf{R} , except that $\bar{r}_{jk} = r_{jk} - \zeta r_{jk}$ for $j = 1, 2, \dots, i$. By setting $\zeta = \lfloor r_{ik}/r_{ii} \rfloor$, we ensure $|\bar{r}_{ik}| \leq \bar{r}_{ii}/2$.

To meet the second condition in (6) permutations are needed in the reduction process. Suppose that $\delta r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{k,k}^2$ for some k . Then we interchange columns $k-1$ and k of \mathbf{R} . After the permutation the upper triangular structure of \mathbf{R} is no longer maintained. But we can bring \mathbf{R} back to an upper triangular matrix by using the Gram-Schmidt orthogonalization technique (see [10]) or by a Givens rotation:

$$\bar{\mathbf{R}} = \mathbf{G}_{k-1,k} \mathbf{R} \mathbf{P}_{k-1,k}, \quad (7)$$

where $\mathbf{G}_{k-1,k}$ is an orthogonal matrix and $\mathbf{P}_{k-1,k}$ is a permutation matrix, and

$$\begin{aligned} \bar{r}_{k-1,k-1}^2 &= r_{k-1,k}^2 + r_{k,k}^2, \\ \bar{r}_{k-1,k}^2 + \bar{r}_{k,k}^2 &= r_{k-1,k-1}^2. \end{aligned} \quad (8)$$

Note that the above operation guarantees $\delta \bar{r}_{k-1,k-1}^2 < \bar{r}_{k-1,k}^2 + \bar{r}_{k,k}^2$ since $\delta \leq 1$. The LLL reduction algorithm is described Algorithm 1, where the final reduced upper triangular matrix is still denoted by \mathbf{R} .

After the LLL reduction (4), the ILS problem (3) is then transformed to:

$$\min_{\mathbf{z} \in \mathbb{Z}^n} \|\bar{\mathbf{y}} - \bar{\mathbf{R}} \mathbf{z}\|_2^2, \quad (9)$$

where $\bar{\mathbf{y}} = \bar{\mathbf{Q}}^T \tilde{\mathbf{y}}$ and $\mathbf{z} = \mathbf{Z}^{-1} \mathbf{x}$.

The LLL-reduction is a powerful preprocessing tool that allows to reduce the complexity of search process for finding the ILS solution, see, e.g., [6, 2].

Algorithm 1 LLL reduction

```
1: compute the QR factorization:  $\mathbf{A} = \mathbf{Q} \begin{bmatrix} \mathbf{R} \\ \mathbf{0} \end{bmatrix}$ ;
2: set  $\mathbf{Z} = \mathbf{I}_n$ ,  $k = 2$ ;
3: while  $k \leq n$  do
4:   apply IGT  $\mathbf{Z}_{k-1,k}$  to reduce  $r_{k-1,k}$ :  $\mathbf{R} = \mathbf{R}\mathbf{Z}_{k-1,k}$ ;
5:   update  $\mathbf{Z}$ :  $\mathbf{Z} = \mathbf{Z}\mathbf{Z}_{k-1,k}$ ;
6:   if  $\delta r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{kk}^2$  then
7:     permute and triangularize  $\mathbf{R}$ :  $\mathbf{R} = \mathbf{G}_{k-1,k} \mathbf{R} \mathbf{P}_{k-1,k}$ ;
8:     update  $\mathbf{Z}$ :  $\mathbf{Z} = \mathbf{Z} \mathbf{P}_{k-1,k}$ ;
9:      $k = k - 1$ , when  $k > 2$ ;
10:  else
11:    for  $i = k - 2, \dots, 1$  do
12:      apply IGT  $\mathbf{Z}_{ik}$  to reduce  $r_{ik}$ :  $\mathbf{R} = \mathbf{R}\mathbf{Z}_{ik}$ ;
13:      update  $\mathbf{Z}$ :  $\mathbf{Z} = \mathbf{Z}\mathbf{Z}_{i,k}$ ;
14:    end for
15:     $k = k + 1$ ;
16:  end if
17: end while
```

3 Success Probability of the Babai point and a lower bound

The first integer point found by the Schnorr-Euchner search algorithm [14] for solving (3) is the Babai point \mathbf{x}^B [3], which is defined as follows:

$$\begin{aligned} c_n &= \tilde{y}_n / r_{nn}, \quad x_n^B = \lfloor c_n \rfloor, \\ c_i &= (\tilde{y}_i - \sum_{j=i+1}^n r_{ij} x_j^B) / r_{ii}, \quad x_i^B = \lfloor c_i \rfloor, \end{aligned} \tag{10}$$

for $i = n, n-1, \dots, 1$. Note that the entries of \mathbf{x}^B are determined from the last to the first.

Before we give a formula of the success probability of the Babai point, we would like to introduce Teunissen's result given in [16]. It is easy to verify that the ILS problem in (2) is equivalent to

$$\min_{\mathbf{x} \in \mathbb{Z}^n} (\mathbf{x} - \mathbf{x}^{RLS})^T \mathbf{W}^{-1} (\mathbf{x} - \mathbf{x}^{RLS}), \tag{11}$$

where $\mathbf{x}^{RLS} = (\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T \mathbf{y}$ is the real LS estimator of the integer parameter vector $\hat{\mathbf{x}}$ in (1) and $\mathbf{W} = \sigma^2 (\mathbf{A}^T \mathbf{A})^{-1}$ is its error covariance matrix. In the GPS literature, the form (11) is often used instead of (2). Let \mathbf{W} have the LDL^T factorization: $\mathbf{W} = \mathbf{L} \mathbf{D} \mathbf{L}^T$, where \mathbf{L} is unit lower triangular and \mathbf{D} is diagonal. Then based on this factorization, the Babai point, which is referred to as the Bootstrapping estimator by Teunissen can be generated. Unlike \mathbf{x}^B , the entries of this Babai point are determined from the first to the last due to the form of the factorization of \mathbf{W} . The formula of the success probability of this Babai point given in [16] is $\prod_{i=1}^n \frac{2}{\sqrt{2\pi}} \int_0^{1/(2\sqrt{d_{ii}})} \exp(-\frac{1}{2}t^2) dt$, where d_{ii} is the diagonal entries of \mathbf{D} .

Given \mathbf{A} and \mathbf{y} in the linear model (1), it is more computationally efficient and reliable to compute the QR factorization of \mathbf{A} than to compute the LDL^T factorization of $(\mathbf{A}^T \mathbf{A})^{-1}$ in finding the ILS estimator of $\hat{\mathbf{x}}$ in (1). In the following we give a formula for the success probability of this Babai point \mathbf{x}^B . For the sake of readability, we give a proof, which is easier to follow than the proof given in [16] for the formula mentioned in the previous paragraph.

Theorem 1 Suppose $\tilde{\mathbf{y}} \sim \mathcal{N}(\mathbf{R}\hat{\mathbf{x}}, \sigma^2 \mathbf{I})$ in the ILS problem (3). Let P_B denote the success probability of the Babai point \mathbf{x}^B given in (10), i.e., $P_B = P(\mathbf{x}^B = \hat{\mathbf{x}})$. Then

$$P_B = \prod_{i=1}^n \phi(r_{ii}), \quad \phi(\zeta) = \sqrt{\frac{2}{\pi}} \int_0^{\frac{\zeta}{2\sigma}} \exp(-\frac{1}{2}t^2) dt. \quad (12)$$

Proof. By the chain rule of conditional probabilities:

$$\begin{aligned} P_B &= P(\mathbf{x}^B = \hat{\mathbf{x}}) = P\left(\bigcap_{i=1}^n ([c_i] = \hat{x}_i)\right) \\ &= P([c_n] = \hat{x}_n) \prod_{i=1}^{n-1} P([c_i] = \hat{x}_i | [c_{i+1}] = \hat{x}_{i+1}, \dots, [c_n] = \hat{x}_n). \end{aligned} \quad (13)$$

Since $\tilde{\mathbf{y}} \sim \mathcal{N}(\mathbf{R}\hat{\mathbf{x}}, \sigma^2 \mathbf{I})$,

$$\tilde{y}_n \sim \mathcal{N}(r_{nn}\hat{x}_n, \sigma^2), \quad \tilde{y}_i \sim \mathcal{N}(r_{ii}\hat{x}_i + \sum_{k=i+1}^n r_{ik}\hat{x}_k, \sigma^2), \quad i = n-1, n-2, \dots, 1.$$

Thus,

$$\begin{aligned} c_n &= \tilde{y}_n / r_{nn} \sim \mathcal{N}(\hat{x}_n, \sigma^2 / r_{nn}^2), \\ c_i &= (\tilde{y}_i - \sum_{j=i+1}^n r_{ij}[c_j]) / r_{ii} \sim \mathcal{N}(\hat{x}_i, \sigma^2 / r_{ii}^2), \text{ if } [c_{i+1}] = \hat{x}_{i+1}, \dots, [c_n] = \hat{x}_n. \end{aligned}$$

Then it follows that

$$\begin{aligned} P([c_n] = \hat{x}_n) &= \frac{1}{\sqrt{2\pi} \frac{\sigma}{r_{nn}}} \int_{-\frac{1}{2}}^{\frac{1}{2}} \exp(-\frac{t^2}{2(\frac{\sigma}{r_{nn}})^2}) dt \\ &= \frac{2}{\sqrt{2\pi}} \int_0^{\frac{r_{nn}}{2\sigma}} \exp(-\frac{1}{2}t^2) dt = \phi(r_{nn}). \end{aligned}$$

Similarly, we can obtain

$$P([c_i] = \hat{x}_i | [c_{i+1}] = \hat{x}_{i+1}, \dots, [c_n] = \hat{x}_n) = \phi(r_{ii}).$$

Then from (13) we can conclude that (12) holds. \square

The success probability P_{ILS} of the ILS estimator depends on its Voronoi cell [6] and it is difficult to rigorously compute it because the shape of Voronoi cell is complicated. In [6] a lower bound $F(\frac{d_{\min}^2}{4\sigma^2}, n)$ is proposed to approximate it, where d_{\min} is the length of the shortest lattice vector, i.e., $d_{\min} = \min_{\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^n} \|\mathbf{R}\mathbf{x}\|_2$, and F is the cumulative distribution function of chi-square distribution. However, no polynomial-time algorithm has been found to compute d_{\min} . To overcome this problem, [6] proposed a more practical lower bound $F(\frac{r_{\min}^2}{4\sigma^2}, n)$, where $r_{\min} \equiv \min_i r_{ii}$. Note that P_B is a lower bound on P_{ILS} (see [17]). The following result shows P_B is sharper than $F(\frac{r_{\min}^2}{4\sigma^2}, n)$.

Theorem 2

$$F\left(\frac{r_{\min}^2}{4\sigma^2}, n\right) \leq P_B.$$

Proof. Let $\mathbf{u} \sim \mathcal{N}(\mathbf{0}, \mathbf{I}_n)$. Thus u_1, u_2, \dots, u_n are i.i.d. and $\sum_{i=1}^n u_i^2$ follows the chi-squared distribution with degree n . Let events $E = \{\sum_{i=1}^n u_i^2 \leq \frac{r_{\min}^2}{4\sigma^2}\}$ and $E_i = \{u_i^2 \leq \frac{r_{ii}^2}{4\sigma^2}\}$ for $i = 1, 2, \dots, n$. Since $r_{\min} \leq r_{ii}$, $E \subseteq \bigcap_{i=1}^n E_i$. Thus,

$$\begin{aligned} F\left(\frac{r_{\min}^2}{4\sigma^2}, n\right) &= P(E) \leq P\left(\bigcap_{i=1}^n E_i\right) = \prod_{i=1}^n P(E_i) \\ &= \prod_{i=1}^n \frac{1}{\sqrt{2\pi}} \int_{-\frac{r_{ii}}{2\sigma}}^{\frac{r_{ii}}{2\sigma}} \exp\left(-\frac{1}{2}t^2\right) dt \\ &= \prod_{i=1}^n \phi(r_{ii}) = P_B. \end{aligned}$$

□

In the following, we give an extreme example to show that $F\left(\frac{r_{\min}^2}{4\sigma^2}, n\right)$ can be much smaller than P_B .

Example 1 Let $\mathbf{R} = \begin{bmatrix} 0.001 & 0 \\ 0 & 10 \end{bmatrix}$ and $\sigma = 0.5$. By simple calculations, we obtain $F\left(\frac{r_{\min}^2}{4\sigma^2}, n\right)/P_B = \frac{1}{1596}$. Although this is a contrived example, where the signal-to-noise ratio is very small, it shows that P_B can be much sharper than $F\left(\frac{r_{\min}^2}{4\sigma^2}, n\right)$ as a lower bound on P_{ILS} .

4 Enhancement of P_B by the LLL reduction

In this section we rigorously prove that the LLL reduction algorithm can enhance the success probability P_B of the Babai point.

Suppose we have the QRZ factorization (4), where $\bar{\mathbf{Q}}$ is orthogonal and \mathbf{Z} is unimodular (we do not assume that $\bar{\mathbf{R}}$ is LLL reduced unless we state otherwise). Then with $\bar{\mathbf{y}} = \bar{\mathbf{Q}}^T \tilde{\mathbf{y}}$ and $\mathbf{z} = \mathbf{Z}^{-1} \mathbf{x}$ the ILS problem (3) can be transformed to (9). For (9) we can also define its corresponding Babai point \mathbf{z}^B . This Babai point can be used as an estimator of $\hat{\mathbf{z}} \equiv \mathbf{Z}^{-1} \hat{\mathbf{x}}$, or equivalently $\mathbf{Z} \mathbf{z}^B$ can be used as an estimator of $\hat{\mathbf{x}}$. In (3) $\tilde{\mathbf{y}} \sim \mathcal{N}(\mathbf{R} \hat{\mathbf{x}}, \sigma^2 \mathbf{I})$. It is easy to verify that in (9) $\bar{\mathbf{y}} \sim \mathcal{N}(\bar{\mathbf{R}} \hat{\mathbf{z}}, \sigma^2 \mathbf{I})$. In the following we look at how the success probability of the Babai point changes after some specific transformation of \mathbf{R} .

The following result shows that if the Lovász condition (6) is not satisfied, after a column permutation and triangularization, the success probability of the Babai point increases.

Lemma 1 Suppose that $\delta r_{k-1, k-1}^2 > r_{k-1, k}^2 + r_{kk}^2$ for some k for the \mathbf{R} matrix in the ILS problem (3). After the permutation of columns $k-1$ and k and triangularization, \mathbf{R} becomes $\bar{\mathbf{R}}$, i.e., $\bar{\mathbf{R}} = \mathbf{G}_{k-1, k} \mathbf{R} \mathbf{P}_{k-1, k}$ (see (7)). Then with $\bar{\mathbf{y}} = \mathbf{G}_{k-1, k}^T \tilde{\mathbf{y}}$ and $\mathbf{z} = \mathbf{P}_{k-1, k}^{-1} \mathbf{x}$, (3) can be transformed to (9). Denote $\hat{\mathbf{z}} \equiv \mathbf{P}_{k-1, k}^{-1} \hat{\mathbf{x}}$. Then the Babai \mathbf{z}^B has a success probability greater than or equal to the Babai point \mathbf{x}^B , i.e.,

$$P(\mathbf{x}^B = \hat{\mathbf{x}}) \leq P(\mathbf{z}^B = \hat{\mathbf{z}}), \quad (14)$$

where the equality holds if and only if $r_{k-1, k} = 0$.

Proof. By Theorem 1, what we need to show is the following inequality:

$$\prod_{i=1}^n \phi(r_{ii}) \leq \prod_{i=1}^n \phi(\bar{r}_{ii}). \quad (15)$$

Since $\bar{r}_{ii} = r_{ii}$ for $i \neq k-1, k$, we only need to show

$$\phi(r_{k-1,k-1})\phi(r_{kk}) \leq \phi(\bar{r}_{k-1,k-1})\phi(\bar{r}_{kk}),$$

which is equivalent to

$$\begin{aligned} & \int_0^{\frac{r_{k-1,k-1}}{2\sigma}} \exp(-\frac{1}{2}t^2)dt \int_0^{\frac{r_{kk}}{2\sigma}} \exp(-\frac{1}{2}t^2)dt \\ & \leq \int_0^{\frac{\bar{r}_{k-1,k-1}}{2\sigma}} \exp(-\frac{1}{2}t^2)dt \int_0^{\frac{\bar{r}_{kk}}{2\sigma}} \exp(-\frac{1}{2}t^2)dt. \end{aligned} \quad (16)$$

Since $\mathbf{G}_{k-1,k}$ is orthogonal and $\mathbf{P}_{k-1,k}$ is a permutation matrix, the absolute value of the determinant of the submatrix $\mathbf{R}_{k-1:k,k-1:k}$ is unchanged, i.e., we have

$$r_{k-1,k-1}r_{kk} = \bar{r}_{k-1,k-1}\bar{r}_{kk}. \quad (17)$$

Let

$$a = \frac{r_{k-1,k-1}}{2\sigma} \frac{r_{kk}}{2\sigma} = \frac{\bar{r}_{k-1,k-1}}{2\sigma} \frac{\bar{r}_{kk}}{2\sigma}, \quad (18)$$

$$f(\zeta) = \ln \int_0^\zeta \exp(-\frac{1}{2}t^2)dt + \ln \int_0^{a/\zeta} \exp(-\frac{1}{2}t^2)dt. \quad (19)$$

Then (16) is equivalent to

$$f\left(\frac{\max\{r_{k-1,k-1}, r_{kk}\}}{2\sigma}\right) \leq f\left(\frac{\max\{\bar{r}_{k-1,k-1}, \bar{r}_{kk}\}}{2\sigma}\right). \quad (20)$$

Obviously, if $r_{k-1,k} = 0$, then the equality of (20) holds since in this case $\frac{\max\{r_{k-1,k-1}, r_{kk}\}}{2\sigma} = \frac{\max\{\bar{r}_{k-1,k-1}, \bar{r}_{kk}\}}{2\sigma}$. So we only need to show if $r_{k-1,k} \neq 0$, then the strictly inequality of (20) holds. In the following, we assume $r_{k-1,k} \neq 0$.

From $\delta r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{kk}^2$ and (8) we can conclude that

$$r_{kk}, \bar{r}_{k-1,k-1}, \bar{r}_{kk} < r_{k-1,k-1}.$$

Then, with (18) it follows that

$$\frac{\max\{r_{k-1,k-1}, r_{kk}\}}{2\sigma} = \frac{r_{k-1,k-1}}{2\sigma} > \frac{\max\{\bar{r}_{k-1,k-1}, \bar{r}_{kk}\}}{2\sigma} \geq \sqrt{a}.$$

Thus, to show the strictly inequality of (20) holds, it suffices to show that when $\zeta > \sqrt{a}$, $f(\zeta)$ is a strictly monotonically decreasing function or equivalently $f'(\zeta) < 0$.

From (19),

$$\begin{aligned} f'(\zeta) &= \frac{\exp(-\frac{1}{2}\zeta^2)}{\int_0^\zeta \exp(-\frac{1}{2}t^2)dt} - \frac{\frac{a}{\zeta^2} \exp(-\frac{(\frac{a}{\zeta})^2})}{\int_0^{\frac{a}{\zeta}} \exp(-\frac{1}{2}t^2)dt} \\ &= \frac{1}{\zeta} \left(g(\zeta) - g\left(\frac{a}{\zeta}\right) \right), \end{aligned}$$

where $g(\zeta) = \frac{\zeta \exp(-\frac{1}{2}\zeta^2)}{\int_0^\zeta \exp(-\frac{1}{2}t^2)dt}$. Note that $\zeta > \sqrt{a}$, $\zeta > a/\zeta$. Thus, in order to show $f'(\zeta) < 0$ for $\zeta > \sqrt{a}$, we need only to show that $g(\zeta)$ is a strictly monotonically decreasing function or equivalently $g'(\zeta) < 0$ when $\zeta > 0$.

Simple calculations give

$$g'(\zeta) = \frac{\exp(-\frac{1}{2}\zeta^2)}{(\int_0^\zeta \exp(-\frac{1}{2}t^2)dt)^2} \left[(1 - \zeta^2) \int_0^\zeta \exp(-\frac{1}{2}t^2)dt - \zeta \exp(-\frac{1}{2}\zeta^2) \right].$$

If $1 - \zeta^2 \leq 0$ and $\zeta > 0$, then obviously $g'(\zeta) < 0$. If $1 - \zeta^2 > 0$ and $\zeta > 0$, since $\exp(-\frac{1}{2}t^2) \leq 1$,

$$(1 - \zeta^2) \int_0^\zeta \exp(-\frac{1}{2}t^2)dt \leq \zeta(1 - \zeta^2) < \zeta \exp(-\frac{1}{2}\zeta^2),$$

where the second inequality can easily be verified. Thus again $g'(\zeta) < 0$ when $\zeta > 0$, completing the proof. \square

Now we make some remarks. The above proof shows that $f(\zeta)$ for $\zeta \geq \sqrt{a}$ reaches its minimum when $\zeta = \sqrt{a}$. Thus if $\bar{r}_{k-1,k-1} = \bar{r}_{kk}$, P_B will increase most.

In Lemma 1 there is no requirement that $r_{k-1,k}$ should be the size-reduced. The question we would like to ask here is do size reductions in the LLL reduction algorithm affect P_B ? From (12) we observe that P_B only depends on the diagonal entries of \mathbf{R} . Thus size reductions *alone* will not change P_B . However, if a size reduction can bring changes to the diagonal entries of \mathbf{R} after a permutation, then it will affect P_B . Therefore, all the size reductions on the off diagonal entries above the superdiagonal have no any effect on P_B . But the size reductions on the superdiagonal entries may affect P_B . There are a few different situations.

Suppose that the Lovász condition (6) holds for a specific k . If (6) does not hold any more after the size reduction on $r_{k-1,k}$, then columns $k-1$ and k of \mathbf{R} are permuted by the LLL reduction algorithm and according to Lemma 1 P_B increases. If (6) still holds after the size reduction on $r_{k-1,k}$, then this size reduction does not affect P_B .

Suppose the Lovász condition (6) does not hold for a specific k . Then by Lemma 1 P_B increases after a permutation and triangularization. If $|r_{k-1,k}| > r_{k-1,k-1}/2$, in the next lemma, we show that the size reduction on $r_{k-1,k}$ performed before the permutation can increase P_B further.

Lemma 2 Suppose that in the ILS problem (3) \mathbf{R} satisfies $\delta r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{kk}^2$ and $|r_{k-1,k}| > r_{k-1,k-1}/2$ for some k . Let $\bar{\mathbf{R}}, \bar{\mathbf{y}}, \mathbf{z}$ and $\hat{\mathbf{z}}$ be defined as in Lemma 1. Suppose a size reduction on $r_{k-1,k}$ is performed first and then after the permutation of columns $k-1$ and k and triangularization, \mathbf{R} becomes $\hat{\mathbf{R}}$, i.e., $\hat{\mathbf{R}} = \hat{\mathbf{G}}_{k-1,k} \mathbf{R} \mathbf{Z}_{k-1,k} \mathbf{P}_{k-1,k}$. Let $\hat{\mathbf{y}} = \hat{\mathbf{G}}_{k-1,k}^T \bar{\mathbf{y}}$ and $\mathbf{w} = \mathbf{P}_{k-1,k}^{-1} \mathbf{Z}_{k-1,k}^{-1} \mathbf{x}$, then (3) is transformed to $\min_{\mathbf{w} \in \mathbb{Z}^n} \|\hat{\mathbf{y}} - \hat{\mathbf{R}}\mathbf{w}\|_2$. Denote $\hat{\mathbf{w}} = \mathbf{P}_{k-1,k}^{-1} \mathbf{Z}_{k-1,k}^{-1} \hat{\mathbf{x}}$. Then the Babai \mathbf{w}^B corresponding to the new transformed ILS problem has a success probability greater than or equal to the Babai point \mathbf{z}^B , i.e.,

$$P(\mathbf{z}^B = \hat{\mathbf{z}}) \leq P(\mathbf{w}^B = \hat{\mathbf{w}}), \quad (21)$$

where the equality holds if and only if

$$|r_{k-1,k-1}r_{k-1,k}| = r_{k-1,k}^2 + r_{kk}^2. \quad (22)$$

Proof. Obviously it suffices to show that

$$\phi(\bar{r}_{k-1,k-1})\phi(\bar{r}_{kk}) \leq \phi(\hat{r}_{k-1,k-1})\phi(\hat{r}_{kk}),$$

which, by the proof of Lemma 1, is equivalent to

$$f(\max\{\bar{r}_{k-1,k-1}, \bar{r}_{kk}\}) \leq f(\max\{\hat{r}_{k-1,k-1}, \hat{r}_{kk}\}),$$

where f is defined in (19). Since $f(\zeta)$ has been showed to be strictly monotonically decreasing when $\zeta > \sqrt{a}$. what we need to show is

$$\max\{\bar{r}_{k-1,k-1}, \bar{r}_{kk}\} \geq \max\{\hat{r}_{k-1,k-1}, \hat{r}_{kk}\}, \quad (23)$$

and the equality holds if and only if (22) holds.

Since $|r_{k-1,k}| > r_{k-1,k-1}/2$,

$$\begin{aligned}\bar{r}_{k-1,k-1} &= \sqrt{r_{k-1,k}^2 + r_{kk}^2} > \sqrt{r_{k-1,k-1}^2/4 + r_{kk}^2}, \\ \bar{r}_{kk} &= \frac{r_{k-1,k-1}r_{kk}}{\sqrt{r_{k-1,k}^2 + r_{kk}^2}} < \frac{r_{k-1,k-1}r_{kk}}{\sqrt{r_{k-1,k-1}^2/4 + r_{kk}^2}}.\end{aligned}$$

But $\sqrt{r_{k-1,k-1}^2/4 + r_{kk}^2} \geq \frac{r_{k-1,k-1}r_{kk}}{\sqrt{r_{k-1,k-1}^2/4 + r_{kk}^2}}$, thus

$$\max\{\bar{r}_{k-1,k-1}, \bar{r}_{kk}\} = \bar{r}_{k-1,k-1}.$$

Suppose that after the size reduction, $r_{k-1,k}$ becomes $\tilde{r}_{k-1,k}$. Note that

$$\hat{r}_{k-1,k-1} = \sqrt{\tilde{r}_{k-1,k}^2 + r_{kk}^2} < \sqrt{r_{k-1,k}^2 + r_{kk}^2} = \bar{r}_{k-1,k-1}.$$

Thus, it follows from (23) what we need to prove is $\hat{r}_{kk} \leq \bar{r}_{k-1,k-1}$ or equivalently

$$\hat{r}_{kk} \leq \sqrt{r_{k-1,k}^2 + r_{kk}^2}, \quad (24)$$

and the equality holds if and only if (22) holds.

By the conditions given in the lemma, $|r_{k-1,k}| < r_{k-1,k-1} < 2|r_{k-1,k}|$. Thus

$$\begin{aligned}\tilde{r}_{k-1,k} &= r_{k-1,k} - \lfloor r_{k-1,k}/r_{k-1,k-1} \rfloor r_{k-1,k-1} \\ &= r_{k-1,k} - \text{sign}(r_{k-1,k})r_{k-1,k-1}.\end{aligned}$$

If $r_{k-1,k} > 0$, then

$$\begin{aligned}\hat{r}_{kk} &= \frac{r_{k-1,k-1}r_{kk}}{\hat{r}_{k-1,k-1}} = \frac{r_{k-1,k-1}r_{kk}}{\sqrt{\tilde{r}_{k-1,k}^2 + r_{kk}^2}} \\ &= \frac{r_{k-1,k-1}r_{kk}}{\sqrt{(r_{k-1,k} - r_{k-1,k-1})^2 + r_{kk}^2}}.\end{aligned}$$

Thus it suffices to show

$$\frac{r_{k-1,k-1}r_{kk}}{\sqrt{(r_{k-1,k} - r_{k-1,k-1})^2 + r_{kk}^2}} \leq \sqrt{r_{k-1,k}^2 + r_{kk}^2}.$$

Simple algebraic manipulations shows that the above inequality is equivalent to

$$(r_{k-1,k-1}r_{k-1,k} - r_{k-1,k}^2 - r_{kk}^2)^2 \geq 0,$$

which certainly holds. And obviously, the equality in (24) holds, if and only if

$$r_{k-1,k-1}r_{k-1,k} = r_{k-1,k}^2 + r_{kk}^2.$$

If $r_{k-1,k} < 0$, we can similarly prove (24) holds and the equality holds if and only if

$$-r_{k-1,k-1}r_{k-1,k} = r_{k-1,k}^2 + r_{kk}^2,$$

completing the proof. \square

From Lemmas 1 and 2 we immediately obtain the following results.

Theorem 3 Suppose that the ILS problem (3) is transformed to the ILS problem (9), where $\bar{\mathbf{R}}$ is obtained by Algorithm 1. Then

$$P(\mathbf{x}^B = \hat{\mathbf{x}}) \leq P(\mathbf{z}^B = \hat{\mathbf{z}}),$$

where the equality holds if and only if no column permutation occurs during the LLL reduction process or whenever two consecutive, say $k-1$ and k , columns are permuted, $r_{k-1,k} = 0$. Any size reductions on the superdiagonal entries of \mathbf{R} which is immediately followed by a column permutation during the LLL reduction process will enhance the success probability of the Babai point. All other size reductions have no any effect on the success probability of the Babai point.

Now we make some remarks. Note that the LLL reduction is not unique. Two different LLL reduction algorithms may produce different \mathbf{R} . In Algorithm 1, when the Lovász condition for two consecutive columns is not satisfied, then a column permutation takes places to ensure the Lovász condition to be satisfied. If an algorithm which computes the LLL reduction does not do permutations as Algorithm 1 does, e.g., the algorithm permutes two columns which are not consecutive or permutes two consecutive columns but the corresponding Lovász condition is not satisfied after the permutation, then we cannot guarantee this specific LLL reduction will increase P_B .

It is interesting to note that [11] showed that all the size reductions on the off diagonal entries above the superdiagonal of \mathbf{R} have no any effect on the residual norm of the Babai point. Here we see that those side reductions are not useful from another perspective.

By Lemma 1, a column permutation of \mathbf{R} can increase P_B . A large δ is likely to increase the chances of column permutations and so increase P_B . Let \mathbf{A} have the QRZ factorization $\mathbf{Q}_i^T \mathbf{A} \mathbf{Z}_i = \begin{bmatrix} \mathbf{R}_i \\ \mathbf{0} \end{bmatrix}$, where \mathbf{R}_1 and \mathbf{R}_2 are δ_1 -LLL reduced and δ_2 -LLL reduced, respectively, and $\delta_1 < \delta_2$. Note that \mathbf{R}_2 must be δ_1 -LLL reduced, but \mathbf{R}_1 may not be δ_2 -LLL reduced. If \mathbf{R}_2 can be obtained by applying the LLL reduction algorithm (with $\delta = \delta_2$) to \mathbf{R}_1 , then by Theorem 3 the success probability of the Babai point corresponding to \mathbf{R}_2 should be at least as large as the success probability of the Babai point corresponding to \mathbf{R}_1 . However, the conclusion may not hold in general if \mathbf{R}_1 and \mathbf{R}_2 were obtained by applying the LLL reduction algorithm with $\delta = \delta_1$ and $\delta = \delta_2$ respectively to \mathbf{A} . The reason is the LLL reduction is not unique. We use an example to illustrate this.

Example 2 Let

$$\mathbf{A} = \begin{bmatrix} 0.9675 & 0.4328 & 0.0935 & 0.9477 \\ 0 & 0.5879 & 0.6792 & 0.4456 \\ 0 & 0 & 0.4295 & 0.0549 \\ 0 & 0 & 0 & 0.0853 \end{bmatrix}.$$

Applying Algorithm 1 to \mathbf{A} with $\delta = \delta_1 = \frac{4}{9}$ and $\delta = \delta_2 = \frac{25}{36}$, we obtain δ_1 -LLL reduced \mathbf{R}_1 and δ_2 -LLL reduced \mathbf{R}_2 , respectively:

$$\mathbf{R}_1 = \begin{bmatrix} 0.4852 & 0.0678 & -0.0232 & -0.1236 \\ 0 & -0.3485 & -0.0578 & 0.1235 \\ 0 & 0 & -0.3413 & 0.0990 \\ 0 & 0 & 0 & -0.3612 \end{bmatrix},$$

$$\mathbf{R}_2 = \begin{bmatrix} 0.5549 & -0.2591 & 0.1280 & -0.0001 \\ 0 & 0.3845 & -0.1278 & -0.0855 \\ 0 & 0 & 0.2960 & -0.0996 \\ 0 & 0 & 0 & 0.3299 \end{bmatrix}.$$

Note that \mathbf{R}_1 is not δ_2 LLL reduced. Applying Algorithm 1 to \mathbf{R}_1 with $\delta = \delta_2$, we obtain δ_2 -LLL reduced $\hat{\mathbf{R}}_2$:

$$\hat{\mathbf{R}}_2 = \begin{bmatrix} 0.3550 & 0.0523 & -0.1448 & 0.0926 \\ 0 & 0.3429 & -0.0889 & -0.0470 \\ 0 & 0 & 0.3767 & -0.1346 \\ 0 & 0 & 0 & -0.4544 \end{bmatrix}.$$

Let $\sigma = 0.1$, then we have

$$P_B(\mathbf{R}_1) = 0.7665, \quad P_B(\mathbf{R}_2) = 0.7295, \quad P_B(\hat{\mathbf{R}}_2) = 0.7756.$$

Obviously, $P_B(\mathbf{R}_2) < P_B(\mathbf{R}_1) < P_B(\hat{\mathbf{R}}_2)$.

5 Reduction of the search complexity by the LLL reduction

In this section, we rigorously show that applying the LLL reduction algorithm can reduce the computational complexity of sphere decoders, which is measured approximately by the number of nodes in the search tree.

The complexity results of sphere decoders given in the literature are often about the complexity of enumerating all integer points in the search region:

$$\|\tilde{\mathbf{y}} - \mathbf{R}\mathbf{x}\|_2 \leq \beta, \quad (25)$$

where β is a constant called the search radius. A typical measure of the complexity is the number of nodes enumerated by sphere decoders, which we denote by ζ .

For $i = n, n-1, \dots, 1$, define E_i as follows

$$E_i = |\{\mathbf{x}_{i:n} \in \mathbb{Z}^{n-i+1} : \|\tilde{\mathbf{y}}_{i:n} - \mathbf{R}_{i:n,i:n}\mathbf{x}_{i:n}\|_2 \leq \beta\}|. \quad (26)$$

As given in [13], E_i can be estimated as follows:

$$E_i \approx \frac{V_{n-i+1} \beta^{n-i+1}}{|\det(\mathbf{R}_{i:n,i:n})|} = \frac{V_{n-i+1} \beta^{n-i+1}}{|r_{ii}r_{i+1,i+1} \cdots r_{nn}|}, \quad (27)$$

where V_{n-i+1} denotes the volume of an $(n-i+1)$ -dimensional unit Euclidean ball. This estimation would become the expected value to E_i if $\tilde{\mathbf{y}}_{i:n}$ is uniformly distributed over a Voroni cell of the lattice generated by $\mathbf{R}_{i:n,i:n}$. Then we have (see, e.g., [1, Sec 3.2] and [15]).

$$\zeta = \sum_{i=1}^n E_i \approx \hat{\zeta}(\mathbf{R}) \equiv \sum_{i=1}^n \frac{V_{n-i+1} \beta^{n-i+1}}{r_{ii}r_{i+1,i+1} \cdots r_{nn}}. \quad (28)$$

In practice, when a search decoder such as the Schnorr-Euchner algorithm is used in the search process, after an integer point is found, β will be updated to shrink the search region. But ζ or $\hat{\zeta}$ here do not take this into account for the sake of simplicity.

The following result shows that if the Lovász condition (6) is not satisfied, after a column permutation and triangularization, the complexity $\hat{\zeta}(\mathbf{R})$ decreases.

Lemma 3 Suppose that $\delta r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{kk}^2$ for some k for the \mathbf{R} matrix in the ILS problem (3). After the permutation of columns $k-1$ and k and triangularization, \mathbf{R} becomes $\bar{\mathbf{R}}$, i.e., $\bar{\mathbf{R}} = \mathbf{G}_{k-1,k} \mathbf{R} \mathbf{P}_{k-1,k}$ (see (7)). Then the complexity $\hat{\zeta}(\mathbf{R})$ of the search process decreases after the transformation, i.e.,

$$\hat{\zeta}(\mathbf{R}) > \hat{\zeta}(\bar{\mathbf{R}}). \quad (29)$$

Proof. Since $\bar{r}_{ii} = r_{ii}$ for $i \neq k-1, k$, $\bar{r}_{k-1,k-1}\bar{r}_{kk} = r_{k-1,k-1}r_{kk}$, and $\bar{r}_{kk} > r_{kk}$, we have

$$\begin{aligned}\hat{\zeta}(\mathbf{R}) - \hat{\zeta}(\bar{\mathbf{R}}) &= \sum_{i=1}^n \frac{V_{n-i+1} \beta^{n-i+1}}{r_{ii}r_{i+1,i+1} \cdots r_{nn}} - \sum_{i=1}^n \frac{V_{n-i+1} \beta^{n-i+1}}{\bar{r}_{ii}\bar{r}_{i+1,i+1} \cdots \bar{r}_{nn}} \\ &= \frac{V_{n-k+1} \beta^{n-k+1}}{r_{kk}r_{k+1,k+1} \cdots r_{nn}} - \frac{V_{n-k+1} \beta^{n-k+1}}{\bar{r}_{kk}r_{k+1,k+1} \cdots r_{nn}} \\ &= \left(\frac{1}{r_{kk}} - \frac{1}{\bar{r}_{kk}} \right) \frac{V_{n-k+1} \beta^{n-k+1}}{r_{k+1,k+1} \cdots r_{nn}} > 0.\end{aligned}$$

□

Suppose the Lovász condition (6) does not hold for a specific k and furthermore $|r_{k-1,k}| > r_{k-1,k-1}/2$. The next lemma, which is analogous to Lemma 2, shows that the size reduction on $r_{k-1,k}$ performed before the permutation can decrease the complexity $\hat{\zeta}(\mathbf{R})$ further.

Lemma 4 Suppose that in the ILS problem (3) \mathbf{R} satisfies $\delta r_{k-1,k-1}^2 > r_{k-1,k}^2 + r_{kk}^2$ and $|r_{k-1,k}| > r_{k-1,k-1}/2$ for some k . Let $\bar{\mathbf{R}}$ be defined as in Lemma 3. Suppose a size reduction on $r_{k-1,k}$ is performed first and then after the permutation of columns $k-1$ and k and triangularization, \mathbf{R} becomes $\hat{\mathbf{R}}$, i.e., $\hat{\mathbf{R}} = \hat{\mathbf{G}}_{k-1,k} \mathbf{R} \mathbf{Z}_{k-1,k} \mathbf{P}_{k-1,k}$. Then

$$\hat{\zeta}(\bar{\mathbf{R}}) > \hat{\zeta}(\hat{\mathbf{R}}). \quad (30)$$

Proof. By the same argument given in the proof of Lemma 3, we have

$$\hat{\zeta}(\bar{\mathbf{R}}) - \hat{\zeta}(\hat{\mathbf{R}}) = \left(\frac{1}{\bar{r}_{kk}} - \frac{1}{\hat{r}_{kk}} \right) \frac{V_{n-k+1} \beta^{n-k+1}}{r_{k+1,k+1} \cdots r_{nn}}.$$

To show (30) we need only to prove $\bar{r}_{kk} < \hat{r}_{kk}$. Since $\bar{r}_{k-1,k-1}\bar{r}_{kk} = \hat{r}_{k-1,k-1}\hat{r}_{kk}$ and $\hat{r}_{k-1,k-1} < \bar{r}_{k-1,k-1}$ (see (??) in the proof of Lemma 2), we have $\bar{r}_{kk} < \hat{r}_{kk}$, completing the proof. □

From Lemmas 3 and 4 we immediately obtain the following result.

Theorem 4 Suppose that the ILS problem (3) is transformed to the ILS problem (9), where $\bar{\mathbf{R}}$ is obtained by Algorithm 1. Then

$$\hat{\zeta}(\mathbf{R}) \geq \hat{\zeta}(\bar{\mathbf{R}}),$$

where the equality holds if and only if no column permutation occurs during the LLL reduction process. Any size reductions on the superdiagonal entries of \mathbf{R} which is immediately followed by a column permutation during the LLL reduction process will reduce the complexity $\hat{\zeta}$. All other size reductions have no any effect on $\hat{\zeta}$.

The about result on the effect of the size reductions is consistent with a result given in [19], which shows that all the size reductions on the off-diagonal entries above the superdiagonal of \mathbf{R} and the size reductions on the superdiagonal entries of \mathbf{R} which are not followed by column permutations have no any effect on the search speed of the Schnorr-Euchner algorithm for finding the ILS solution.

6 Summary and future work

We have shown that the success probability P_B of the Babai point will increase and the complexity $\hat{\zeta}$ of sphere decoders will decrease if the LLL reduction algorithm given in Algorithm 1 is applied for lattice reduction. In addition, we have shown that P_B is a better lower bound on the success probability of ILS estimator than the lower bound given in [6].

The implementation of LLL reduction is not unique. The KZ reduction [9] is also an LLL reduction. But the KZ conditions are stronger than the LLL conditions. Whether some implementations of the KZ reduction can always increase P_B and decrease $\hat{\zeta}$ will be studied in the future.

References

- [1] W. ABEDISEID, *Efficient Lattice Decoders for the Linear Gaussian Vector Channel: Performance & Complexity Analysis*, PhD thesis, Department of Electrical and Computer Engineering, University of Waterloo, 2011.
- [2] E. AGRELL, T. ERIKSSON, A. VARDY, AND K. ZEGER, *Closest point search in lattices*, IEEE Transactions on Information Theory, 48 (2002), pp. 2201–2214.
- [3] L. BABAI, *On Lovasz lattice reduction and the nearest lattice point problem*, Combinatorica, 6 (1986), pp. 1–13.
- [4] M. O. DAMEN, H. E. GAMAL, AND G. CAIRE, *On maximum likelihood detection and the search for the closest lattice point*, IEEE Transactions on Information Theory, 49 (2003), pp. 2389–2402.
- [5] Y. H. GAN AND W. H. MOW, *Novel joint sorting and reduction technique for delay-constrained LLL-aided MIMO detection*, IEEE Signal Processing Letter, 15 (2008), pp. 194–197.
- [6] A. HASSIBI AND S. BOYD, *Integer parameter estimation in linear models with applications to GPS*, IEEE Transactions on Singal Processing, 46 (1998), pp. 2938–2952.
- [7] J. JALDÉN, L. BARBERO, B. OTTERSTEN, AND J. THOMPSON, *The error probability of the fixed-complexity sphere decoder*, IEEE Transactions on Singal Processing, 57 (2009), pp. 2711–2720.
- [8] J. JALDÉN AND B. OTTERSTEN, *On the complexity of sphere decoding in digital communications*, IEEE Transactions on Signal Processing, 53 (2005), pp. 1474–1484.
- [9] A. KORKINE AND G. ZOLOTAREFF, *Sur les formes quadratiques*, Mathematische Annalen, 6 (1873), pp. 366–389.
- [10] A. LENSTRA, H. LENSTRA, AND L. LOVÁSZ, *Factoring polynomials with rational coefficients*, Mathematische Annalen, 261 (1982), pp. 515–534.
- [11] C. LING AND N. HOWGRAVE-GRAHAM, *Effective LLL reduction for lattice decoding*, in IEEE International Symposium on Information Theory, 2007, IEEE, 2007, pp. 196–200.
- [12] D. MICCIANCIO, *The hardness of the closest vector problem with preprocessing*, IEEE Transactions on Information Theory, 47 (2001), pp. 1212–1215.
- [13] J. M. W. P. M. GRUBER, ed., *Handbook of convex geometry*, North-Holland, Amsterdam, 1993.
- [14] C. SCHNORR AND M. EUCHNER, *Lattice basis reduction: improved practical algorithms and solving subset sum problems*, Mathematical Programming, 66 (1994), pp. 181–191.
- [15] D. SEETHALER, J. JALDÉN, C. STUDER, AND H. BÖLCSKEI, *On the complexity distribution of sphere decoding*, IEEE Transactions on Information Theory, 57 (2011), pp. 5754–5768.
- [16] P. J. G. TEUNISSEN, *Success probability of integer GPS ambiguity rounding and bootstrapping*, Journal of Geodesy, 72 (1998), pp. 606–612.
- [17] —, *An optimality property of integer least-squares estimator*, Journal of Geodesy, 73 (1999), pp. 587–593.
- [18] P. VAN EMDE BOAS, *Another NP-complete partition problem and the complexity of computing short vectors in a lattice.*, tech. report, Technical report 81-04, Mathematics Department, University of Amsterdam, 1981.

- [19] X. XIE, X. CHANG, AND M. AL BORNO, *Partial LLL reduction*, in Proceedings of IEEE GLOBE-COM 2011, 5 pages, 2011.
- [20] P. XU, *Voronoi cells, probabilistic bounds, and hypothesis testing in mixed integer linear models*, IEEE Transactions on Information Theory, 52 (2006), pp. 3122–3138.